# INTEGRATION OF DIGITAL SIGNATURES

# INTO THE EUROPEAN BUSINESS REGISTER

*Helmut Kurth*

Industrieanlagen Betriebsgesellschaft mbH
Einsteinstr. 20
D-85521 Ottobrunn, Germany

kurth@iabg.de

## Abstract:

In the INFOSEC programme 1994 the European Union set up three trial projects to demonstrate the feasibility of the use of digital signatures in pan-European networks. One of those trials was the EBRIDGE project, where customers could extract the official business register data from companies of four European countries on-line and authenticated by digital signatures. Authenticated data from those official business registers has to be presented in some European countries to notaries or banks for specific types of contracts. Today the common way to obtain this data in an authenticated form is to get an officially signed copy of the business register data by surface mail. Since it may take up to two weeks to obtain this information in this conventional way, some contracts where delayed by this time and financial losses could be the result of this delay. With the infrastructure established in the EBRIDGE project, the official business register data can be obtained digitally signed in a few seconds. In addition, the EBRIDGE projects demonstrated that the official business registers could also serve as Trusted Third Parties by maintaining public keys of company representatives and distribute them in a secure way.

## Introduction

In 1994 the European Union set up the INFOSEC'94 programme which had the main objective to demonstrate the use of digital signatures and trusted third party services in pan-European trade. Three projects where started covering different aspects that are needed to establish a Public Key Infrastructure in Europe. One of those projects was the EBRIDGE project, which integrated digital signature technology into the prototype of the European Business Register. The European Business Register tries to link the official business register data bases of the countries within the European Union and makes this data available by an on-line services.

In all European countries, each company has to register itself to an official authority before it can start to operate. Entering data into and changing data in those business registers is performed by authorized personal only (e. g. notaries). Data in this register contains among others: the name and address of the company, the legal status of the company, the names of persons allowed to sign contracts on behalf of the company and additional information about the business areas and some financial information about the company. These official business registers play an important role for trade in Europe. Many countries demand that for specific types of contracts the a signed copy of the official business register data for all companies involved in the contract has to be obtained and attached to the contract. Banks

often also request such a signed copy of the business register data for credits. Obtaining manually signed copies of the business register information is time consuming, can slow down business and may even result in lost business opportunities.

In 1993 four European countries (Denmark, France, Italy and the UK) started a project to make their official business register data available on-line and link those databases together. This project was called the European Business Register (EBR) project and was funded by the European Union under the ENS programme. It was soon recognized that on-line access to business register information without a proof of authenticity of this information was not sufficient. Therefore in 1994 the EBRIDGE project was started to enhance the EBR prototype by integrating digital signatures. The partners within this project were: Mercury (UK), Cerved (Italy), OR-Telematique (France) and DCCA (Denmark) as the Service Broker in the four countries that run the EBR trial, Sema Group (UK) as project coordinator, Denton Hall (UK) and ISTEV (Italy) dealing with the legal aspects, IABG (Germany) leading the security architecture design and implementation and Siemens Austria who provided the digital signature software.

## Overall architecture

The European Business Register (EBR) provides a European Union-wide public service for the retrieval of officially registered information concerning European companies. It has established a running prototype network that currently includes four European countries (France, UK, Italy and Denmark). In each country there is a service broker, who provides the on-line access to the local business register data. EBR interlinked those national service broker thereby allowing customers to access business register data from all four countries.

Figure 1 provides an overview over the current structure of the EBR.

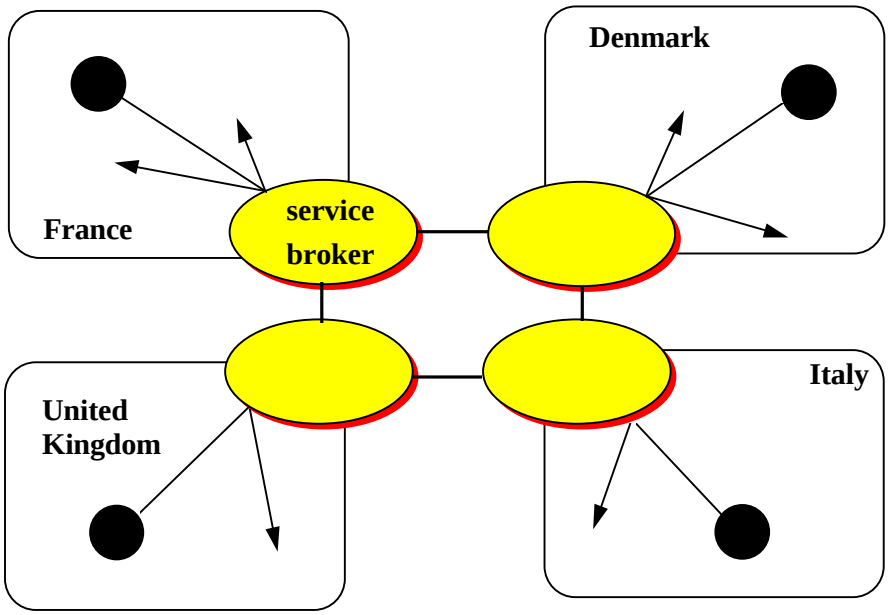


**Figure 1: EBR Service Infrastructure**

The figure shows that each customer contacts only his national service broker, which extracts information from other countries via the EBR network and transforms it to the presentation style

specific its own customers. Each service broker has a direct link to a national on-line registry database system. These database systems are the sources of all retrieved information. The service broker are interlinked using an X.25 network. A proprietary protocol was designed on top of X.25 for the information exchange between service brokers.

The goal of the EBRIDGE project was, to provide the customers of EBR with the possibility to prove the authenticity of the business register data. Several problems had to be solved within the project:

- The structure and content of the business register data bases in the four countries is different due to the different laws concerning the business registers in each country.

- Since the electronic business registers had been developed separately, different query languages are used in the different countries.

- Query results from other countries have to be transformed into the national presentation style. Since different languages are used in the four countries, field names and the content of some fields has to be translated before it is presented to a customer in another country.

This requires that the query as well as the data resulting from the query has to be transformed on its transmission path. Since this transformation would invalidate the digital signature applied by the originating service broker, the data has to be re-signed by the local service broker before the data is transferred to the customer. To maintain the chain of trust from the customer to the originating service broker, the local service broker maintains an audit trail of all signed data he received from a foreign service broker. The data he re-signs and transmits to his customer contain a 'link field', which points to the audit record of the original data he has received from the foreign service broker. In case of a dispute, he can immediately extract the signed original data from the audit trail and put the responsibility for the correctness of the information on the originating service broker. This general architecture is shown in figure 2.

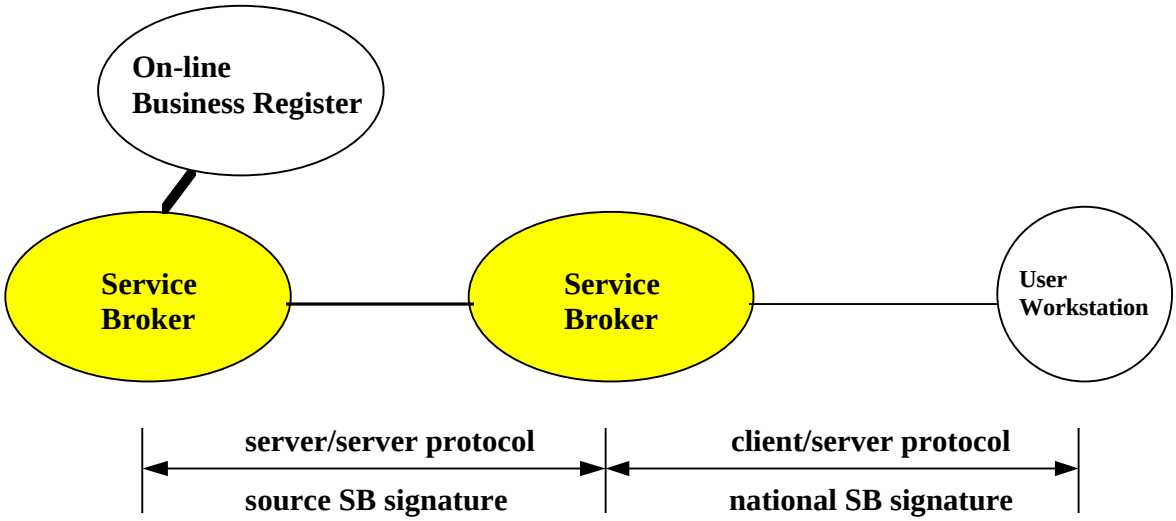


**Figure 2: Service Broker Signature Functions**

Each service broker domain consists of several systems serving different purposes:

- A service broker host (usually a large mainframe system) which contains the business register data base

- A Unix based machine, called the 'Portable Service Broker System' (PSBS), which interconnects the different service broker systems via a X.25 based network

- A special 'Protected Electronic Signature Machine' (PESM) operating in a protected environment which generates and verifies digital signatures.

The Portable Service Broker Machine was specifically developed to allow other nations to join the EBR easily. This machine provides a simple adaptable interface to the service broker host to allow the integration of different types of host and their database systems to be integrated into the EBR network. The system was developed on a Unix basis and can be ported easily to different Unix based platforms.

The Protected Electronic Signature Machine was also developed on a Unix basis. The Unix operating system was specifically configured and extended to allow secure operation. The specific features of the Protected Electronic Signature Machine are described in more detail later in this paper.

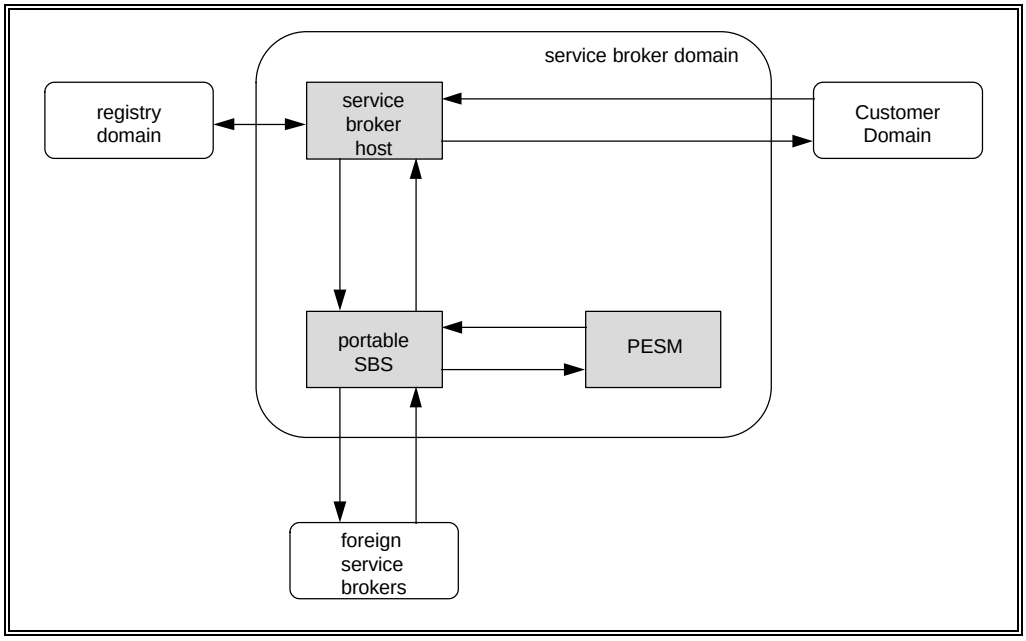


**Figure 3: Structure Of A Service Broker System**

A simplified form of the flow of information resulting from a user's request is shown in figure 4. The sequence of information flow is shown in the diagram by the numbered arrows.

The user is the originator of all requests for service. A service request may specify the delivery of signed or unsigned information. The request itself is not signed. Requests for delivery of signed information are handled in the following way. Information is signed before transmission by the SBS providing the information and the signature is verified upon receipt by the SBS requesting the information on behalf of the user. This second SBS then transforms and re-signs the information and forwards it to the user workstation. This extends the chain of trust backwards, giving both the user and the local SBS confidence that the company information has not been modified since it was signed

after retrieval from the distant business register – and did indeed come from the appropriate service broker. A user's trust depends upon the local SBS having an appropriate level of security to protect the international transfers and so the service brokers have to be trusted.

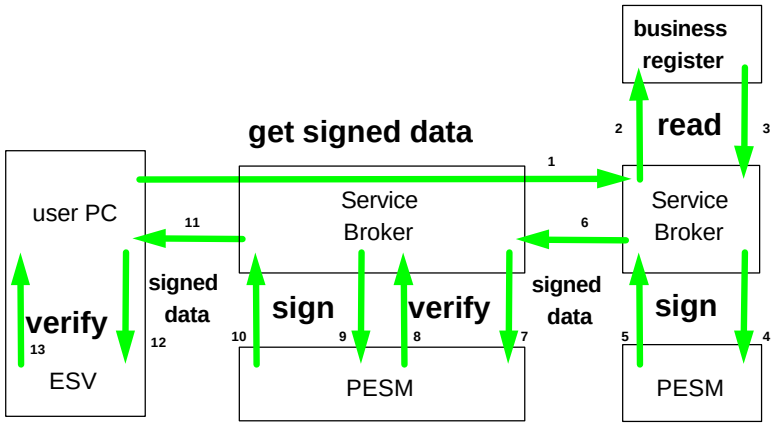


**Figure 4: Flow of Information in the EBRIDGE Architecture**

To explain the semantics of the arrows in figure 4, we take the example of a UK customer, who wants to obtain authenticated business register data of an Italian company.

1. The user submits the query request to the UK service broker. The UK service broker transmits the request (after transformation to the Italian request format) to the Italian service broker.

2. The Italian service broker submits the request to the Italian business register database.

3. The reply from the Italian business register database is sent back to the Italian service broker.

4. The Italian service broker sends the data to his Protected Electronic Signature Machine to digitally sign the data.

5. The data and the signature are passed back to the Italian service broker system.

6. The signed data is then transmitted to the UK service broker.

7. The UK service broker submits the signed data to his Protected Electronic Signature Machine to verify the signature of the Italian service broker.

8. The PESM tells the service broker system, if the signature was successfully verified.

9. When the signature was verified successfully, the service broker system writes the signed data to an audit trail and transforms the data received according to his national presentation scheme. Then the transformed data is sent to the PESM to be signed by the UK service broker.

10. The PESM of the UK service broker signs the data and passes data and signature back to the UK service broker system.

11. The UK service broker system passes the data to the customer, who has submitted the request.

12. The customer locally verifies the signature of the UK service broker.

13. After successful verification of the signature, data and signature are stored in the customer's system.

For the EBRIDGE service signatures are created using a one-way hash function (MD5) and asymmetric encryption (RSA). Key pairs are generated within the PESMs at each site. Private keys are isolated within these PESMs. Each service broker has to pass its public keys to each other service broker and each service broker has to distribute its own public key to its local national terminal population. A specific protocol has been implemented to allow the service broker to change their key pair. The certificate passed with each signed information contains the date of issue of the key used to sign a document. Whenever a customer or a foreign service broker detects that he does not have the current public key of a service broker, he may issue a request to submit the new public key. The service broker then submits the new public key signed with his 'Master Key'. Since this master key is used only to distribute the new public key, a longer key length can be used for this key (e. g. 2048 bit). This and the fact that only few messages are signed with this key reduces the possibility of a cryptographic attack against this key.

The other crucial element in the EBRIDGE architecture is a trusted audit trail. Each service broker maintains an audit log containing records of received signed information. Information forwarded to a customer contains a reference to a specific record in the audit log of the local SBS. In the event of a problem or dispute these audit logs can be used to determine the point in the delivery chain at which the problem arose, so identifying responsibility for problem resolution.

## The Protected Electronic Signature Machine

As a result of the risk analysis undertaken in the beginning of the project it was decided to have a separated Protected Electronic Signature Machine instead of maintaining the private keys in a general purpose machine to which many people may have access. Separating the electronic signature functions from all other parts of the application allows for a high level of physical and procedural protection which minimizes the risk that the private keys are compromised or that the critical software is tampered with. The design of the PESM allows to concentrate all the critical hardware and software components of a service broker in a single machine which performs only the security critical actions of the service broker. Only a limited number of persons must have physical access to the machine.

The operating system of the PESM is Unix. It was chosen because it can be configured in a way which restricts each user of the PESM to only those functions he needs for his operational role. The PESM supports only three operational roles:

### System Administrator

### Key Administrator

### Auditor

The Unix system is configured in way which prohibits that any user can log in as root or obtain root privileges. Only users with one of the special application defined roles mentioned above are allowed

to log into the system. If additional maintenance actions have to be performed, the operating system has to be reconfigured thereby deleting the critical data stored in the system. Backup procedures for this data exist, which automatically encrypt the backup medium. Two persons with different roles (System Administrator and key Administrator) are needed for backup and restore where each person defines a part of the key used for encryption. The encrypted keys on the backup medium are of course integrity protected.

Each user is assigned one of the roles mentioned above. For each role a restricted shell has been developed which will allow each role to execute only those commands necessary for their task. None of these roles will directly get superuser privileges. All actions which require special privileges (e. g. adding new users or changing a user account) will be performed by setuid-protected programs. Especially all actions of the key administrator will be performed in a way which prohibits that the key administrator has direct access to the private keys stored in the machine. This has the advantage that although the Key Administrator is able to generate a new key pair on the PESM, he is not able to read the private key he has generated.

An audit function is installed which logs each attempted login as well as each command issued by a System Administrator or a Key Administrator. This audit log is maintained by the Auditor and can not be accessed by either a System Administrator or a Key Administrator.

These functions and features ensure that the PESM can be operated securely. But of course these functions need to be complemented by physical protection, procedural measures and measures to assure that the security critical software in the PESM is implemented correctly and has no security critical side effects. The physical and procedural protection features are described in a System Security Plan that has been produced as part of the project. This plan states all the measures that are assumed to be sufficient for the provision of a very high level of security as required by a commercial service. In addition a pre-evaluation using the ITSEC and ITSEM was performed for the critical application software of the PESM.

## Conclusion

The EBRIDGE project demonstrated the use of digital signatures for the on-line access of data from official registers in a field trial, that was conducted in the summer of 1995. The functions can be seen as a prototype for the on-line access to other types of registries containing data that has to be authenticated. In addition the EBRIDGE project can be a starting point for a Public Key Infrastructure for commercial business in Europe. If the public keys of persons authorized to sign contracts on behalf of a company are stored as part of the data in the official business registers the EBRIDGE system would provide the service brokers with the ability to act as a Certification Authority for those public keys. No new infrastructure is needed for this purpose.

Technically the EBRIDGE project has solved the problems to establish a part of a Public Key Infrastructure that can be used to for Electronic Trade in Europe. But currently the legal situation is not yet prepared for such a system. Digital signatures are not yet accepted as equivalent to hand written signatures and the legal status of the official business registers is not identical in each European country. But with the demonstration of the feasibility of integrating digital signatures and Trusted Third Party services in an existing infrastructure the EBRIDGE project pushed the demand for a solution to the legal problems.

The EBRIDGE project is just one example of several projects the EU has funded to establish a base for electronic trade in Europe. Other projects in this area are the projects FAST, BOLERO, TESTFIT and CAFE. Within it's new ACTS programme the EU has started two other projects (SEMPER and FANS) that will help to establish a working public key infrastructure that can be used for electronic trade in Europe.

Also the legal situation is beginning to change. In several countries new laws are under discussion which set up the legal framework for the acceptance of digital signatures. E. g. in Germany a proposal for such a law has been distributed to technical and legal experts for discussion. This proposed law contains also several technical requirements regarding the security of the systems operated by a Trusted Third Party as well as the security of the user equipment that generates the digital signature. The technical security requirements for systems operated by TTPs fit well with the features implemented in the PESM within the EBRIDGE project.

## References

[1] INFOSEC'94 Workplan, Commission of the European Union, July 1993

[2] S2201 EBR ES&TTP Phase 1 Final Report, EBRIDGE Project, May 1994

[3] FAST II Project Description, Philips, April 1994

[4] EBRIDGE ES&TTP Enhancement to EBR, Final Report, EBRIDGE Project, August 1995